



Deutscher**Anwalt**Verein

Stellungnahme

**des Deutschen Anwaltvereins vorbereitet durch
die Ausschüsse Recht der Inneren Sicherheit,
Informationsrecht und Strafrecht**

**zum Referentenentwurf eines Gesetzes zur
Einführung einer IP-Adressspeicherung**

Stellungnahme Nr.: 8/2026

Berlin, im Januar 2026

Mitglieder des Ausschusses Recht der Inneren Sicherheit

- Rechtsanwältin Lea Voigt, Bremen (Vorsitzende)
- Rechtsanwalt Wilhelm Achelpöhl, Münster
- Rechtsanwalt Dr. David Albrecht, Berlin
- Rechtsanwältin Dr. Lea Babucke, Düsseldorf
- Rechtsanwalt Dr. Eren Basar, Düsseldorf
- Prof. Dr. Annika Dießner, Berlin (ständiges Gastmitglied im Ausschuss)
- Rechtsanwalt Dr. Nikolas Gazeas, LL.M., Köln
- Rechtsanwalt Dr. Andreas Grözing, Köln
- Rechtsanwalt Dr. Mayeul Hiéramente, Hamburg
- Rechtsanwalt Dr. Saleh Ihwas, Frankfurt am Main
- Rechtsanwältin Dr. Regina Michalke, Frankfurt am Main
- Prof. Dr. Mark A. Zöller, München (ständiges Gastmitglied im Ausschuss, Berichterstatter)

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwalt Max Gröning, Geschäftsführer, Berlin
- Rechtsanwältin Katharina Schmidt-Matthäus, Referentin, Berlin

Mitglieder des Ausschusses Informationsrecht

- Rechtsanwalt Prof. Niko Härting, Berlin (Vorsitzender, Berichterstatter)
- Rechtsanwalt Dr. Simon Assion, Frankfurt
- Rechtsanwältin Dr. Christiane Bierekoven, Düsseldorf
- Rechtsanwältin Isabell Conrad, München
- Rechtsanwalt Prof. Dr. Malte Grützmaker, LL.M., Hamburg
- Rechtsanwalt Peter Huppertz, LL.M, Düsseldorf
- Rechtsanwalt Dr. Helmut Redeker, Bonn
- Rechtsanwältin Dr. Kristina Schreiber, Köln (Berichterstatterin)
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwältin Nicole Narewski, Geschäftsführerin, Berlin

Mitglieder des Ausschusses Strafrecht

- Rechtsanwalt Stefan Conen, Berlin
- Rechtsanwältin Dr. Friederike Goltsche, Münster
- Rechtsanwältin Dr. Gina Greeve, Frankfurt am Main
- Rechtsanwalt Kai Kempgens, Berlin (Berichterstatter)
- Rechtsanwalt Prof. Dr. Stefan Kirsch, Frankfurt am Main
- Rechtsanwältin Dr. Jenny Lederer, Essen
- Rechtsanwalt Prof. Dr. Bernd Müssig, Bonn
- Rechtsanwalt Prof. Dr. Ali B. Norouzi, Berlin (Vorsitzender)
- Rechtsanwältin Dr. Anna Oehmichen, Berlin
- Rechtsanwältin Gül Pinar, Hamburg (Stellv. Vorsitzende)
- Rechtsanwalt Prof. Dr. Tilman Reichling, Frankfurt am Main
- Rechtsanwalt Martin Rubbert, Berlin

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwältin Tanja Brexl, Geschäftsführerin, Berlin
- Michael Bimmler, Referent, Berlin

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV versammelt ca. 60.000 Rechtsanwältinnen und Rechtsanwälte sowie Anwaltsnotarinnen und Anwaltsnotare, die in 253 lokalen Anwaltvereinen im In- und Ausland organisiert sind. Er vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene. Der DAV ist im Lobbyregister für die Interessenvertretung gegenüber dem Deutschen Bundestag und der Bundesregierung zur Registernummer R000952 eingetragen.

A. Einführung

Der Gesetzesentwurf sieht für alle deutschen Zugangsprovider eine Fortsetzung der Verpflichtung zur Vorratsdatenspeicherung vor und kombiniert die Vorratsdatenspeicherung mit einem als Sicherungsanordnung bezeichneten Quick-Freeze-Verfahren für andere Verkehrsdaten. Die seit 2010 anhaltende Diskussion über „Quick Freeze“ als Alternative zur Vorratsdatenspeicherung soll damit beendet werden, dass man beide Verfahren einführt und damit in erheblicher Weise in die Grundrechte der Bürgerinnen und Bürger eingreift. Dabei setzt man sich über die europarechtlichen Maßgaben hinweg, die sowohl der Europäische Gerichtshof (EuGH) als auch das Bundesverwaltungsgericht (BVerwG) in den *SpaceNet*-Entscheidungen gesetzt haben. Auch die vermeintliche anschließende Öffnung für die Speicherung von IP-Adressen durch den EuGH in seiner Entscheidung *La Quadrature du Net* u.a. (EuGH EuGRZ 2024, 246) wird in einem Maße überdehnt, die nicht mehr mit den grundrechtsschützenden Intentionen des Gerichtshofs in Einklang steht. Wegen des Fehlens jeglicher wirksamen Begrenzung der Verwendungszwecke ist jedenfalls die vorgeschlagene Vorratsdatenspeicherung europarechtswidrig.

Die geplante Neuregelung senkt die Schwelle für eine der eingriffsintensivsten Ermittlungsmaßnahmen der StPO bedenklich ab. Damit drohen Verkehrsdatenerhebungen, etwa retrograde Standortdaten oder Funkzellendaten von bisherigen Ausnahmeinstrumenten bei schwerster Kriminalität zu regelmäßig einsetzbaren Ermittlungswerkzeugen zu werden. Aus Sicht des Deutschen Anwaltvereins hat dies tiefgreifende Folgen für Unbeteiligte und für das Vertrauen der Bürgerinnen und Bürger in die Vertraulichkeit mobiler Kommunikation.

Mit der voranschreitenden Digitalisierung der Gesellschaft werden die Verkehrsdaten der Bürgerinnen und Bürger immer dichter und aussagekräftiger. Die Kommunikation erfolgte vor wenigen Jahren noch deutlich seltener digital. Selbst durch Überwachung des stationären Telefonverkehrs ließen sich die Bewegungen von Bürgerinnen und Bürgern nicht lückenlos nachverfolgen, Bewegungen im analogen Raum und in der eigenen Wohnung waren nur über Observationen mit (sehr) hohen Eingriffsvoraussetzungen möglich.

Heutzutage ist der digitale Datenverkehr dagegen allgegenwärtig. Die weit überwiegende Zahl der Bürgerinnen und Bürger führt ganztätig ein Mobiltelefon mit sich, das bei Standortänderungen aufgrund der Einwahl in neue Funkmasten Daten hinterlässt. PKWs speichern fortlaufend ebensolche Daten des Fahrzeugführers, die regelmäßig anzutreffenden SOS-Funktionen erzeugen Bewegungsdaten bei den Mobilfunkanbietern. Insgesamt ist das Internet nicht erst seit Corona zum Hauptkommunikationskanal der Menschen gewachsen – zu Hause wie auch im beruflichen Alltag. Konzerttickets, Termine für Arztbesuche, alltägliche Einkäufe und vieles anderes werden heute über das Internet gebucht und durchgeführt. Im Jahr 2026 ist es daher, will man am gesellschaftlichen Leben in irgendeiner Weise teilhaben, unvermeidbar geworden, Spuren im digitalen Raum zu hinterlassen. Zu diesen Spuren zählen die durch die Änderungen im Referentenentwurf (§ 100g StPO) besonders stark betroffenen Verkehrsdaten (darunter fallen z.B. Anrufzeiten, gewählte Rufnummern, IP-Adressen, Standortdaten, Beginn und Ende der Internetverbindung). Zwar sind keine Inhaltsdaten betroffen, bereits Verkehrsdaten lassen aber tiefgehende Einblicke in die private Lebensführung der Nutzenden zu.

Schon allein die staatlich veranlasste Speicherung dieser Daten geht mit einem empfindlichen Grundrechtseingriff einher. Werden die Daten vom Staat erhoben, lässt sich daraus ein Bewegungsprofil erstellen, das Einblicke in die (höchst-)persönliche Lebensgestaltung des Betroffenen zulässt. In der digitalen Gesellschaft sind derartige Maßnahmen von besonders hoher Intensität, denn niemand kann sich ihrer Erhebung entziehen – sie sind aber geeignet, die Lebensführung von Bürgerinnen und Bürgern maßgeblich einzuschränken. Maßnahmen, die ein derartiges Bewegungsprofil zulassen, bedürfen nach der Rechtsprechung des Verfassungsgerichts besonders hoher Eingriffsschwellen (BVerfG 1 BvR 256/08 - Urteil vom 2. März 2010). Der Entwurf

läuft aus Sicht des Deutschen Anwaltvereins vor diesem Hintergrund auch Gefahr, gegen Verfassungsrecht zu verstoßen.

B. Vorratsdatenspeicherung

Durch die geplante Neuregelung soll erneut eine Vorratsdatenspeicherung bei allen Internet-Zugangsprovidern eingeführt werden. Dies ergibt sich bereits aus einem Vergleich zwischen dem bisherigen § 176 Abs. 3 TKG und § 176 Abs. 1 TKG-E. § 176 Abs. 1 Nr. 4 TKG-E erweitert sogar die auf Vorrat zu speichernden Daten um *„die der Internetprotokoll-Adresse zugehörigen Portnummern und weitere Verkehrsdaten, soweit diese für eine Identifizierung des Anschlussinhabers anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse erforderlich sind“*.

Für einen Zugriff auf die bei Internet-Zugangsprovidern gespeicherten IP-Adressen und anderen Metadaten soll es nach § 100j Abs. 2 StPO-E – wie bereits nach bisherigem Recht (§ 100j Abs. 2 StPO) – genügen, dass die Ermittlung des Anschlussinhabers („Bestandsdaten“) „für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten“ benötigt werde. Jede Ermittlungsmaßnahme – gleich um welches Delikt es sich handelt – würde damit eine Identifizierung des Anschlussinhabers ermöglichen. Dies erstaunt, da das BVerwG in seiner *Spacenet*-Entscheidung § 100j Abs. 2 StPO unter Hinweis auf die EuGH-Entscheidung zu *Spacenet* (EuGH vom 20.9.2022 – C-793/19, C-794/19) die Vorratsdatenspeicherung für europarechtswidrig erachtet hat mit der Begründung, es fehle an einer Begrenzung der Verwendungszwecke auf den Schutz der nationalen Sicherheit, die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit (BVerwG vom 14.8.2023, Az. 6 C 6/22 Rn. 42). Vor dem Hintergrund der Rechtsprechung des EuGH und des BVerwG hat der DAV keinen Zweifel an der Europarechtswidrigkeit der unbegrenzten Zugriffsbefugnis nach § 100j Abs. 2 StPO-E.

Die Rechtslage hinsichtlich der Bestandsdatenauskunft soll zudem auch noch durch den Fortfall verfahrensrechtlicher Sicherheiten verschlechtert werden. Die Protokollierungspflicht bei jedem einzelnen Zugriff auf Bestandsdaten (§ 100j Abs. 2 Satz 2 StPO) soll ersatzlos entfallen. Der Zugriff auf die Daten soll jedem im

Polizeidienst tätigen Ermittlungsbeamten möglich sein (§ 101a Abs. 5 StPO-E i.V.m. § 100a Abs. 4 StPO).

Seit der BVerfG-Entscheidung zur Vorratsdatenspeicherung aus dem Jahre 2010 wird das Quick-Freeze-Verfahren als Alternative zur Vorratsdatenspeicherung diskutiert. In dem Gesetzesentwurf der Ampelregierung aus dem Jahr 2024 wurde eine solche Regelung als „Sicherungsanordnung“ bezeichnet. In § 100g Abs. 7 StPO-E findet sich jetzt – zusätzlich zu einer Vorratsdatenspeicherung – das Instrument einer Sicherungsanordnung, das – anders als die Vorratsdatenspeicherung, zu der nur Zugangsprovider verpflichtet sind – für alle TK-Provider und für alle Verkehrsdaten gelten soll. Der Gesetzesentwurf kombiniert somit Vorratsdatenspeicherung und Quick-Freeze. Für die Zugangsprovider bedeutet dies, dass im Falle einer Sicherungsanordnung die Vorratsdaten auch über die dreimonatige Regelfrist hinaus gespeichert bleiben dürfen und müssen (§ 175 Abs. 1 TKG-E).

Die Ausgestaltung der Verarbeitungsbefugnis der TK-Unternehmen in §§ 175 und 176 TKG-E ist in entscheidenden Punkten unbestimmt und bringt so für die verpflichteten Unternehmen erhebliche Rechtsunsicherheiten. Die adressierten TK-Unternehmen müssen einerseits ihre Pflichten aus dem TKG einhalten und andererseits die Rechte ihrer Kundinnen und Kunden schützen. Diese Stellung macht es notwendig, dass die Regelungen zur IP-Adressspeicherung präzise und klar gefasst sind und keinen Auslegungsspielraum zulasten der Normadressaten belassen. Dem genügt insbesondere § 176 TKG-E noch nicht angesichts von unzureichend geregelten Abrufbefugnissen und nur vage vorgegebenen technisch-organisatorischen Schutzmaßnahmen sowie einer pauschalen Speicherfrist von drei Monaten. Die Verkürzung der Neuregelung gegenüber der vorherigen Fassung bringt insofern keine Erleichterungen oder Entbürokratisierung, sondern Rechtsunsicherheit für die Normverpflichteten.

Die Bundesnetzagentur wird zwar mit Überwachungsaufgaben betraut (§§ 175 Abs. 3, 176 Abs. 4 TKG-E), diese sollten indes noch um konkrete Vorgaben zur Durchführung dieser Kontrollen und zur Berichterstattung an die Öffentlichkeit ergänzt werden. Zudem sollte eine Evaluationsklausel aufgenommen werden, die eine Überprüfung der Wirksamkeit und Verhältnismäßigkeit der IP-Adressenspeicherung vorsieht, z.B. nach

drei Jahren. Bei negativer Evaluierung sollte die Regelung automatisch außer Kraft treten. Zudem sollte die Rolle vom Bundesamt für die Sicherheit in der Informationstechnik und der Bundesbeauftragten für Datenschutz angesichts ihrer jeweiligen Kompetenzen ergänzend mit einbezogen werden.

Der Entwurf sieht keine Marginalgrenze oder Erleichterungen für kleine Internetzugangsanbieter vor, was zu einer unverhältnismäßigen Belastung führen könnte. Die Einführung einer Marginalgrenze für Anbieter mit weniger als 10.000 oder 100.000 Kunden sollte erwogen werden. Zudem ist die Schaffung klarer Erstattungsansprüche für Kosten der technischen Umsetzung der Speicherpflicht, gerade zugunsten von kleinen Anbietern, zu prüfen, um unverhältnismäßige Belastungen zu vermeiden. Das JVEG wird insofern nur partiell angepasst, fokussiert auf Auskünfte und Übermittlung von Daten, bislang aber noch nicht im Hinblick auf die Implementierungskosten der technischen Systeme und die Speicherung als solche.

C. Absenkung der Eingriffsschwelle bei der Erhebung von Verkehrsdaten

1. Neuregelung in § 100g StPO

Die bisherige Fassung des § 100g StPO folgte einem ausdifferenzierten Schutzkonzept, das die Zulässigkeit der Verkehrsdatenerhebung an unterschiedliche Eingriffsschwellen bindet. Maßgeblich ist dabei insbesondere eine Unterscheidung nach der Art der erhobenen Daten (Standort-, Funkzellen-, sonstige Verkehrsdaten) und Art der Erhebung der Daten (retrograd vs. fortlaufend).

Demgegenüber führt die Neuregelung zu einer Vermengung bislang klar getrennter Eingriffsformen. Laufende und retrograde Daten gleich welcher Art werden nun weitgehend denselben tatbestandlichen Voraussetzungen unterstellt. Damit wird ohne Not ein System aufgegeben, das der unterschiedlichen Eingriffsintensität der einzelnen Maßnahmen Rechnung trug.

Die Anpassungen würden die Anwendungspraxis im Übrigen kaum vereinfachen. Die Neuregelung entzerrt zwar die unterschiedlichen Eingriffsarten in verschiedene

Absätze; inhaltlich beschränken sich diese jedoch weitgehend auf Verweisungen untereinander, sodass sich die materiellen Eingriffsvoraussetzungen nur noch in begrenztem Umfang unterscheiden. Ein Beispiel: Die Eingriffsvoraussetzungen der Funkzellenabfrage findet der Rechtsanwender in § 100g Abs. 4. Dort steht jedoch nur eine Verweisung auf Absatz 3. In § 100g Abs. 3 (Standortdaten) findet er wiederum ein Verweis auf Absatz 1. Hier sind die einfachen Voraussetzungen einer Erhebung von jeglicher Art von Verkehrsdaten geregelt. Dann wird der Blick des Rechtsanwenders wieder zurück in Absatz 3 wandern, um die Subsidiaritätsklausel zu erfassen. Er muss sich also sämtliche Eingriffsvoraussetzungen aus verschiedenen anderen Absätzen bilden.

Dem Gesetzentwurf nach werde das bestehende Schutzniveau im Wesentlichen beibehalten. Diese Einschätzung überzeugt aus Sicht des Deutschen Anwaltvereins nicht. Die Vereinheitlichung der Voraussetzungen führt zu einer faktischen Absenkung des Schutzstandards. Jede Art von Eingriff nach § 100g StPO wird nun der bisher niedrigsten Schwelle nach Absatz 1 unterstellt.

Wo bislang besonders eingriffsintensive Maßnahmen – etwa die Funkzellenabfrage oder die retrograde Erhebung von Standortdaten – an qualifizierte Katalogtaten gebunden waren, genügt künftig regelmäßig der Verdacht einer Straftat von auch im Einzelfall erheblicher Bedeutung – also der mittleren Kriminalität. Das kann nach der Rechtsprechung des Bundesverfassungsgerichts je nach Fallgestaltung auch eine Beleidigung oder Nötigung sein (BVerfG, Beschluss vom 24. Juli 2013 - 2 BvR 298/12), regelmäßig umfasst dies Straftaten mit einer Höchststrafe von 5 Jahren und mehr, also auch eine einfache Körperverletzung. Dieser Begriff ist daher zu weit und in der Praxis kaum geeignet, die Maßnahme effektiv auf Ausnahmefälle zu begrenzen.

Nach bisheriger Rechtslage war klar umrissen, wegen welcher (schweren) Straftaten ein Verdacht vorliegen muss und wann ein Eingriff in Freiheitsrechte (Persönlichkeitsgrundrecht/Telekommunikationsgrundrecht aus Art. 1 Abs. 1, Art. 2 Abs. 1 GG) gerechtfertigt ist. Der Gesetzesentwurf ersetzt dies mit dem unbestimmten Rechtsbegriff einer „Straftat von im Einzelfall erheblicher Bedeutung“. Das ist in Hinblick auf die erhebliche Eingriffsintensität zu unbestimmt. Die

Schutzfunktion des konkreten Straftatenkatalogs wird im Ergebnis durch Subsidiaritäts- und Verhältnismäßigkeitsprüfungen ersetzt, die der besonderen Eingriffsintensität einzelner Maßnahmen nicht gerecht werden.

a. Streichung des Straftatenkatalogs in § 100g Abs. 2 StPO

Besonders schwer wiegt die ersatzlose Streichung des bisherigen § 100g Abs. 2 StPO. Der dort normierte Straftatenkatalog stellte Normenklarheit und Vorhersehbarkeit sicher, indem er die besonders eingriffsintensiven Formen der Verkehrsdatenerhebung ausdrücklich auf außergewöhnlich schwere Straftaten beschränkte.

Mit dem Wegfall dieses Katalogs entfällt eine objektive, gesetzlich vorgegebene Eingriffsschwelle. An ihre Stelle tritt ein offener, auslegungsbedürftiger Maßstab („Straftat von auch im Einzelfall erheblicher Bedeutung“), der der gerichtlichen Praxis einen erheblichen Spielraum eröffnet. Dies stärkt nicht die Sicherheit für Bürgerinnen und Bürger, sondern vergrößert die Rechtsunsicherheit – sowohl für Betroffene als auch für die Rechtsanwendung.

Gerade bei verdeckten Ermittlungsmaßnahmen, deren Einsatz für Bürgerinnen und Bürger regelmäßig nicht vorhersehbar ist, kommt der Normenklarheit besondere Bedeutung zu. Verdeckte Ermittlungsmaßnahmen werden eben nicht offen, sondern heimlich geführt. Im Gegenzug muss den Bürgerinnen und Bürgern durch eine konkrete Gesetzgebung vor Augen geführt werden, wann ein solcher verdeckter Eingriff erfolgen kann. Bewährt hat sich – im Einklang mit verfassungsrechtlicher Rechtsprechung zum Bestimmtheitsgrundsatz – die Schaffung von abschließenden Straftatenkatalogen (vgl. § 100g Abs. 2 StPO, aber auch § 100a Abs. 2, § 100b Abs. 2 StPO). Ihr Verlust wiegt umso schwerer, als nach der Rechtsprechung des Bundesgerichtshofs das Fehlen einer tragenden gesetzlichen Eingriffsvoraussetzung regelmäßig ein Beweisverwertungsverbot nach sich zieht. Stattdessen wird in § 100g Abs. 1 S. 1 Nr. 1 StPO-E der Kreis der Anlasstaten von auch im Einzelfall erheblicher Bedeutung lediglich durch einen beispielhaften Verweis („insbesondere“) auf den Straftatenkatalog des § 100a Abs. 2 StPO beschrieben. Insofern fehlt es an jeder

Eingrenzungsfunktion des Gesetzgebers für den Rechtsanwender und damit im Ergebnis an der verfassungsrechtlich erforderlichen Bestimmtheit der Regelung.

Im Zusammenspiel mit § 100g Abs. 7 StPO-E setzt der Wegfall des Katalogs einen Normmechanismus in Gang, der gegen die Rechtsprechung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung (BVerfG 1 BvR 256/08 - Urteil vom 2. März 2010, Rn. 228) verstoßen dürfte, wonach ein verbindlicher Straftatenkatalog – der die Eingriffe auf schwerste Straftaten begrenzt – bei Verwendung von Daten aus einer Vorratsdatenspeicherung zwingend erforderlich ist:

*„Für die Strafverfolgung folgt hieraus, dass ein Abruf der Daten zumindest den durch bestimmte Tatsachen begründeten Verdacht **einer schweren Straftat** voraussetzt. **Welche Straftatbestände** hiervon umfasst sein sollen, **hat der Gesetzgeber abschließend** mit der Verpflichtung zur Datenspeicherung **festzulegen**. Ihm kommt hierbei ein Beurteilungsspielraum zu. Er kann dabei entweder auf **bestehende Kataloge zurückgreifen oder einen eigenen Katalog schaffen**, etwa um Straftaten, für die die Telekommunikationsverkehrsdaten besondere Bedeutung haben, zu erfassen. Die Qualifizierung einer Straftat als schwer muss aber in der Strafnorm - insbesondere etwa durch deren Strafraumen - einen objektivierten Ausdruck finden (vgl. BVerfGE 109, 279 <343 ff., insbesondere 347 f.>). Eine Generalklausel oder lediglich **die Verweisung auf Straftaten von erheblicher Bedeutung reichen hingegen nicht aus.**“ (Hervorhebung durch den Verfasser)*

Die Sicherungsanordnung sieht nach § 100g Abs. 7 Satz 2 StPO-E im Ergebnis eine Verwendung von nach § 100g Abs. 7 Satz 1 StPO-E auf Vorrat gespeicherten Daten vor. Denn schon bei einem bloßen Anfangsverdacht können massenhaft Verkehrsdaten – darunter Standortdaten und Daten aus einer Funkzelle – auf bloße Anordnung der Staatsanwaltschaft ohne gerichtliche Prüfung drei Monate lang (§ 101a Abs. 1 Satz 1 Nr. 3a StPO-E) gespeichert werden. Erhoben werden sollen sie dann nach den eingegebenen Voraussetzungen aus § 100g Abs. 1-4 StPO-E bei Straftaten von im Einzelfall

erheblicher Bedeutung und damit gerade ohne einen verbindlichen Straftatenkatalog. Das ist in dieser Form mit der aufgezeigten Linie des Bundesverfassungsgerichts nicht vereinbar.

Die Neuregelung und insbesondere die Streichung des Katalogs des § 100b Abs. 2 StPO birgt damit die Gefahr einer erheblichen Zunahme rechtlich unsicherer Maßnahmen sowie nachfolgender Verwertungsstreitigkeiten. Sie steuert in der derzeitigen Form auf vermeidbare (verfassungs-)rechtliche Streitigkeiten und gerichtliche Auseinandersetzungen zur Auslegung der Eingriffsvoraussetzungen zu.

b. Ausweitung der Standortdatenerhebung (§ 100g Abs. 3 StPO-E)

Nach bisheriger Rechtslage sind die Eingriffsvoraussetzungen für die Standortdatenerhebung danach differenziert, ob es sich um retrograde oder künftig anfallende Daten des Standorts handelt. Der vorgelegte Entwurf sieht darin keine Notwendigkeit mehr und verweist dabei darauf, dass die hohen Anforderungen an eine retrograde Erhebung der Daten in Hinblick auf die Vorratsdatenspeicherung geschaffen worden seien, da damit mehrere Wochen zurückreichenden Bewegungsprofilen erstellt werden könnten. Da diese verfassungswidrig ist, bedürfe es keiner Unterscheidung mehr; eine retrograde Erfassung von Standorten kommt nach derzeitiger Rechtslage nur für Daten in Betracht, die technisch notwendig gespeichert werden (ca. 1 Woche).

Diese Begründung ist jedenfalls vor dem Hintergrund der gleichzeitigen Einführung der Sicherungsanordnung nach § 100g Abs. 7 StPO nicht überzeugend:

Nach der Gesetzesbegründung des derzeitigen § 100g StPO ist „die Erhebung von gespeicherten Standortdaten [ist] besonders sensibel, weil aus ihnen Bewegungsprofile erstellt werden können“ (vgl. Drucksache 18/5088 S. 27). Es spielt keine Rolle, ob diese Bewegungsprofile mehrere Wochen zurückreichen, sondern maßgeblich ist, dass solche Profile (auch mittels eines „nur“ eine Woche zurückreichenden Datensatzes) überhaupt erstellt werden können.

Mit dem sog. „Quick-Freeze“ wird es gemäß § 100g Abs. 7 Satz 1 StPO-E überdies ermöglicht, die Verkehrsdaten (dazu zählen dann auch Standortdaten) bei den verpflichteten Telekommunikationsanbietern auf bloße Anordnung der Staatsanwaltschaft drei Monate lang (ohne gerichtliche Prüfung!) zu speichern (und mit gerichtlichem Beschluss weitere drei Monate) und gemäß Satz 2 nach den Voraussetzungen der § 100g Abs. 1-4 StPO anschließend zu erheben. Senkt man daher in § 100g Abs. 3 die Eingriffsschwelle, so senkt man sie auch für die Erhebung der Daten aus der Sicherungsanordnung. Es wird den Ermittlungsbehörden damit sehr wohl ermöglicht, genau wie bei der Vorratsdatenspeicherung, für einen Zeitraum von bis zu sechs Monaten retrograde Standortdaten zu erheben und detaillierte Bewegungsprofile zu erstellen.

Dies gilt wie erörtert auch für den nach derzeitiger Rechtslage erhebaren Zeitraum von ca. einer Woche. Auch hier lassen sich ohne weiteres Bewegungsprofile erstellen. Daher bedarf es schon nachzeitigem Recht einer hohen Eingriffsschwelle, die mit der Neuregelung in § 100g Abs. 3 StPO-E nicht mehr erreicht werden würde.

Eine derartige Absenkung des Schutzniveaus ist vor diesem Hintergrund aus Sicht des Deutschen Anwaltvereins nicht zu rechtfertigen.

c. Funkzellenabfrage entgegen BGH-Rechtsprechung

Nach zutreffender Rechtsprechung des Bundesgerichtshofs (Beschluss vom 10. Januar 2024 – 2 StR 171/23 Rn. 26) und herrschender Auffassung in der Rechtslehre (vgl. SSW-StPO/Eschelbach, 5. Aufl., § 100g Rn. 38; MüKo-StPO/Rückert, 2. Aufl., § 100g Rn. 87; Singelstein, JZ 2012, 601) bedarf es derzeit auch für die Erhebung von Funkzellendaten gemäß § 100g Abs. 3, 1 Satz 3 StPO einer besonders schweren Straftat aus dem Katalog des § 100g Abs. 2 StPO, da sie wie die Erhebung der retrograden Standortdaten die Erstellung (partieller) Bewegungsprofile ermöglicht. Insoweit ist es überraschend, dass der Entwurf entgegen der eindeutigen höchstrichterlichen Rechtsprechung der Rechtsauffassung von einzelnen Landgerichten den Vorzug geben will.

Ferner ist auf die außergewöhnliche Streubreite der Funkzellenabfrage als zusätzliche Eingriffsqualität hinzuweisen. Das Bundesverfassungsgericht hat in seiner Leitentscheidung zur Vorratsdatenspeicherung (1 BvR 256/08 - Urteil vom 2. März 2010) ausdrücklich betont, dass gerade Maßnahmen mit hoher Streubreite eine besondere Grundrechtsbelastung entfalten. Diese Streubreite ist der Erhebung sämtlicher Daten aus einer Funkzelle stets inhärent. Bei einer Funkzellenabfrage genügt es zu einem ungünstigen Zeitpunkt mit dem Mobiltelefon im Bereich einer bestimmten Funkzelle gewesen zu sein, um in den Zugriffsbereich von strafprozessualen Ermittlungen zu geraten. Diese Gefahr besteht unabhängig davon, ob die Daten später tatsächlich vertieft ausgewertet werden. Allein die Zugriffsbefugnis stellt einen Eingriff in Freiheitsrechte dar. Vor diesem Hintergrund wiegt die im Gesetzentwurf vorgesehene Absenkung der Eingriffsschwelle hier besonders schwer.

So droht eine Verschiebung der Funkzellenabfrage vom Ausnahmeinstrument hin zu einem regelmäßigen Ermittlungsansatz. Die vom Gesetzentwurf angeführte Subsidiaritätsklausel („aussichtslos oder wesentlich erschwert“) vermag diese Entwicklung nicht aufzuhalten. Der Maßstab der „wesentlichen Erschwerung“ ist in der Praxis regelmäßig schnell bejaht und ersetzt keine klar normierte, hohe Eingriffsschwelle. Auf tatsächlicher Ebene wird es dem Betroffenen überdies selten möglich sein, nachzuprüfen oder gar zu belegen, dass eine Funkzellenabfrage nicht erforderlich war, da andere Ermittlungsansätze zur Verfügung standen und dies im Einzelfall so schwer wiegt, dass sich daraus ein Beweisverwertungsverbot ergibt.

Die Eingriffsintensität der Neuregelung muss sich daher nicht allein nach der Tiefe der Information, sondern maßgeblich anhand der Kombination aus Breite und Diffusität der Datenerhebung sowie der fehlenden Begrenzung auf besonders schwere Straftaten messen lassen. In dieser Gesamtschau ist die Funkzellenabfrage in der vorgesehenen Form insbesondere angesichts der Streichung des Katalogs in § 100g Abs. 2 StPO verfassungsrechtlich höchst bedenklich.

d. Ersatzlose Streichung des § 100g Abs. 4 StPO – Schutz von Berufsgeheimnisträgern

Die Regelung zum Schutz von Berufsgeheimnisträgern in § 100g Abs. 4 StPO soll ersatzlos entfallen. Recht knapp heißt es zur Begründung (RefE, S. 28), aus den bei den Zugangsprovidern gespeicherten Daten könnten keine „Erkenntnisse darüber gewonnen werden, mit wem Berufsgeheimnisträger kommuniziert haben“. Dabei wird verkannt, dass Rechtsanwälte, aber auch beispielsweise Journalisten oft gute Gründe haben, zur Ausübung ihrer beruflichen Tätigkeit Internetseiten zu besuchen, auf denen sich rechtswidrige und auch strafbare Inhalte finden. Wenn eine Anwältin ihre Mandanten etwa gegen den Vorwurf von Äußerungsdelikten verteidigen möchte, wird sie womöglich die Seiten entsprechender Chatgruppen aufrufen und läuft damit Gefahr, in das Visier von Strafverfolgungsbehörden zu geraten. Auch eine Kommunikation mit Mandanten in Chatgruppen oder auf Plattformen ist denkbar, die durch den geplanten Fortfall des § 100g Abs. 4 StPO ihren besonderen Schutz verlieren würde. Zudem fällt unter den Schutz des Berufsgeheimnisses bereits das „Ob“ und „Wie“ des Kontakts bzw. der Kontaktaufnahme mit dem Berufsgeheimnisträger. So kann beispielsweise schon die Tatsache, dass ein (potenzieller) Mandant zur Mandatsanbahnung die Telefonnummer des Anwalts auf dessen Kanzleihomepage recherchiert, strafverfolungsrelevante Rückschlüsse zulassen (vgl. BGHSt 36, 301; HK-StPO/Gercke, § 53 Rn. 5; HK-StPO/Zöller, § 160a Rn. 5 m.w.N.).

Der Referentenentwurf verweist zur Begründung der Streichung des speziellen § 100g Abs. 4 StGB auf den zukünftig entfallenden Regelungsbedarf. Der Schutz von Berufsgeheimnisträgern sei nach der allgemeinen Schutzvorschrift des § 160a ausreichend gewährleistet (RefE, S. 28). Die Streichung der bisherigen lex specialis geht jedoch mit einer erkennbaren Absenkung des Schutzniveaus einher. Während sich das bisherige Beweiserhebungsverbot in § 100g Abs. 4 S. 1 StPO auf sämtliche in § 53 Abs. 1 S. 1 Nr. 1 bis 5 StPO genannten Gruppen von Berufsgeheimnisträgern bezieht, sieht § 160a Abs. 1 S. 1 StPO dies nur für die in § 53 Abs. 1 S. 1 Nr. 1, 2 und 4 Benannten (Geistliche, Strafverteidiger und Abgeordnete) sowie Rechtsanwälte und Kammerrechtsbeistände vor. Der Schutz

der übrigen Berufsgeheimnisträger wird nach § 160a Abs. 2 lediglich durch ein relatives Beweisverbot, also faktisch durch eine Abwägung nach Verhältnismäßigkeitserwägungen (HK-StPO/Zöller, § 160a Rn. 11) gewährleistet. Auch das ausdrückliche Verwendungsverbot bzw. Lösungsgebot (vgl. § 100g Abs. 4 S. 5, 160a Abs. 1 S. 5 StPO) in Fällen, in denen berufsgeheimnisbezogene Informationen aus nicht gezielt gegen den Berufsgeheimnisträger gerichteten Maßnahmen erlangt wurden, gilt immer nur für den so bezeichneten Personenkreis. Dieser ist aber im Rahmen von § 160a StPO gegenüber § 100g Abs. 4 deutlich eingeschränkt.

Hinzu kommt, dass der Schutz bereits nach dem geltenden § 100g Abs. 4 StPO unzureichend ausgestaltet ist, da er gegen eine – auch massenhafte – Speicherung und Abfrage von Vorratsdaten, die im Zusammenhang mit der Internetrecherche eines Berufsgeheimnisträgers anfallen, keine ersichtliche Handhabe bietet. Der Deutsche Anwaltverein fordert daher die Bundesregierung auf, im weiteren Verlauf des Gesetzgebungsverfahrens einen deutlich wirksameren Schutz des Berufsgeheimnisses vorzusehen, der jedenfalls das Niveau des bisherigen § 100g Abs. 4 StPO nicht unterschreitet.

2. Einführung der Sicherungsanordnung nach § 100g Abs. 7 StPO-E

Der Entwurf sieht mit § 100g Abs. 7 den sog. „Quick-Freeze“ vor. Damit kann die Staatsanwaltschaft – bei Gefahr im Verzug auch allein ihre Ermittlungsperson (§ 101a Abs. 1 Satz 1 Nr. 3a StPO-E) gegenüber den Verpflichteten (Telekommunikationsanbietern usw.) anordnen, bestimmte Verkehrsdaten fortlaufend zu sichern.

a. Keine Verpflichtung aus dem E-Evidence-Paket der EU

Soweit angeführt wird, aus der Richtlinie (EU) 2023/1544 und der Verordnung (EU) 2023/1543 über die grenzüberschreitende Sicherung und Herausgabe elektronischer Beweismittel in Strafverfahren innerhalb der Europäischen Union ergäbe sich die Notwendigkeit der Einführung einer Sicherungsanordnung in die

Strafprozessordnung, kann dies nicht nachvollzogen werden. Die entsprechende Verordnung verpflichtet die Bundesrepublik, die Voraussetzungen für die zuverlässige Beantwortung eingehender Sicherungsanordnungen anderer EU-Mitgliedsstaaten zu schaffen. Eine Verpflichtung, dieses Ermittlungsinstrument für die eigenen Ermittlungsbehörde zu schaffen, ergibt sich indes nicht aus dem E-Evidence-Paket und wurde folgerichtig auch nicht in den entsprechenden Gesetzesentwurf aufgenommen. Zudem wird verkannt, dass der Erlass einer europäischen Herausgabeanordnung ohnehin immer eine Sicherungsverpflichtung des Adressaten (vgl. Art. 10 Abs. 1 d. VO (EU) 2023/1543) beinhaltet, sodass im hiesigen Strafprozessrecht ohnehin bereits weitergehende Ermächtigungen normiert sind. Das E-Evidence-Paket verfolgt nicht ansatzweise den Zweck, die Mitgliedsstaaten zur Schaffung weitergehender Ermittlungsermächtigungen unter vereinfachten nationalen Voraussetzungen zu veranlassen. Dies liegt ausschließlich in der Entscheidung des hiesigen Gesetzgebers.

b. Niedrige Anordnungsvoraussetzungen

Voraussetzung der Sicherungsanordnung nach § 100g Abs. 7 StPO-E ist ein bloßer Anfangsverdacht einer Straftat (niedrigste denkbare Eingriffsschwelle der StPO), die im Einzelfall erhebliche Bedeutung hat. Das kann nach der Rechtsprechung des Bundesverfassungsgerichts je nach Fallgestaltung schon eine Beleidigung oder Nötigung sein (BVerfG, Beschluss vom 24. Juli 2013 - 2 BvR 298/12), regelmäßig umfasst dies Straftaten mit einer Höchststrafe von 5 Jahren und mehr – also auch eine einfache Körperverletzung. Zweck der Anordnung muss die Aufklärung des Sachverhalts oder die Identifizierung eines möglichen Täters sein. Mehr bedarf es nicht, um einen Normmechanismus in Gang zu setzen, wonach Verkehrsdaten (darunter fallen z.B. Anrufzeiten, gewählte Rufnummern, IP-Adressen, Standortdaten, Beginn und Ende der Internetverbindung) des Betroffenen drei Monate lang – ohne gerichtlichen Beschluss – zunächst gespeichert und wenn sich der Anfangsverdacht zu einem „qualifizierten“ Tatverdacht verdichtet – regelmäßig erhoben werden können. Dieser Zeitraum kann dann mittels gerichtlichen Beschlusses noch um drei weitere Monate verlängert werden, sprich, der Bürger muss damit rechnen, dass

seine Verkehrsdaten bis zu einem halben Jahr gespeichert werden. Konkret gerechtfertigt wird die Länge dieser Maßnahme in der Gesetzesbegründung bisher nicht. Dazu heißt es: *„Die Sicherung darf für einen Zeitraum von höchstens drei Monaten angeordnet werden. Häufig wird dies den Strafverfolgungsbehörden ausreichen, um die Abfragevoraussetzungen herzustellen“* (vgl. RefE S. 41). Eine konkrete Evidenz zur Notwendigkeit dieses Zeitraums wäre begrüßenswert.

c. Eigener Grundrechtseingriff durch Speicheranordnung

Bereits die staatliche Anordnung der Speicherpflicht dürfte unzweifelhaft einen eigenständigen Grundrechtseingriff darstellen. Für die Verletzung der oben genannten Freiheitsrechte kommt es nicht darauf an, ob die Daten auch später verwertet werden. Ein Eingriff liegt bereits in der staatlichen Anordnung der Speicherung, mithin der Überwachung.

Die Sicherungsanordnung dürfte daher in der vorliegenden Form, wie schon unter (1.) ausgeführt, gegen die Rechtsprechung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung (BVerfG 1 BvR 256/08 - Urteil vom 2. März 2010, Rn. 228) verstoßen, wonach ein verbindlicher Straftatenkatalog – der die Eingriffe auf schwerste Straftaten begrenzt – bei Verwendung von Daten aus einer Vorratsdatenspeicherung zwingend erforderlich ist. Die Sicherungsanordnung sieht nach § 100g Abs. 7 Satz 2 StPO-E im Ergebnis eine Verwendung von nach § 100g Abs. 7 Satz 1 StPO-E auf Vorrat gespeicherten Daten ohne abschließenden Katalog für Straftaten auch der mittleren Kriminalität vor. Das ist mit der aufgezeigten Linie des Bundesverfassungsgerichts unvereinbar.

Besonders schwer wiegt zudem das Fehlen eines Richtervorbehalts. Hier besteht in jedem Fall Nachbesserungsbedarf. Soweit in Eilfällen der Staatsanwaltschaft oder ihren Ermittlungspersonen eine Eilkompetenz eingeräumt wird, sollten deren Anordnungen durch das Gericht bestätigt werden müssen. Überdies muss die Einführung des „Quick-Freezes“ zumindest mit einer Beibehaltung des bisherigen Schutzniveaus einhergehen. Das bedeutet, dass Daten aus der Sicherungsanordnung nur dann erhoben werden dürfen, wenn sie zur Verfolgung

von Straftaten nach § 100g Abs. 2 StPO zwingend erforderlich sind, da die gespeicherten (retrograden) Verkehrsdaten stets geeignet sein werden, um Bewegungsprofile zu erstellen.

3. Doppelbelastung durch Kombination mit IP-Adressenvorratsdatenspeicherung

Der Wegfall des bisherigen § 100g Abs. 2 StPO kann nicht isoliert betrachtet werden. Parallel wird eine neue IP-Adressenspeicherpflicht im Telekommunikationsrecht eingeführt, die faktisch eine Form der Vorratsdatenspeicherung darstellt. Die Strafverfolgungsbehörden erhalten dadurch einen breiten verfügbaren Datenbestand, auf den sie über niedrige Eingriffsschwellen praktisch jederzeit und ohne gerichtliche Prüfung zugreifen können. Einen Ausgleich zum Schutz der Bürger sieht der Entwurf an keiner Stelle vor.

In der Gesamtschau führt dies zu einer doppelten Belastung der Freiheitsrechte. Einerseits wird die Zugriffsschwelle für besonders eingriffsintensive Erhebungsvarianten von Verkehrsdaten eingeebnet, andererseits wird der staatlich verfügbare Datenbestand massiv erweitert. Die Kombination beider Elemente verstärkt die Eingriffsintensität erheblich und verschiebt das bisherige Gleichgewicht zwischen effektiver Strafverfolgung und Grundrechtsschutz einseitig und kompensationslos zulasten der Bürgerinnen und Bürger.

4. Neuregelungen in § 100j StPO

Die vorgesehenen Änderungen in § 100j StPO sehen im Wesentlichen nur redaktionelle Anpassungen vor. Nach wie vor können beispielsweise Bestandsdaten zu einer statischen oder dynamischen IP-Adresse durch die Ermittlungsbehörden ohne Richtervorbehalt und ohne qualifizierte Voraussetzungen bei bloßem Vorliegen eines Anfangsverdachts angefordert werden.

Diese Regelung muss im Zusammenhang mit der geplanten IP-Adressenvorratsdatenspeicherung betrachtet werden. Die Eingriffsintensität des § 100j StPO wird hierdurch erheblich gesteigert. Dass das Auskunftersuchen vor diesem Hintergrund unter der niedrigen Eingriffsschwelle nach § 100j Absatz 2 StPO weiterhin als verfassungsgemäß zu betrachten ist, ist aus Sicht des Deutschen Anwaltvereins fraglich.

5. Neuregelungen in § 100k StPO

Die vorgesehenen Änderungen in § 100k StPO sehen einen Gleichlauf mit den Neuregelungen in § 100g StPO-E vor. Insoweit wird entsprechend auf die Ausführungen dazu verwiesen.

6. Neuregelungen in § 101a StPO

Die Änderungen in § 101a StPO sehen zahlreiche Verfahrensregelungen zur Erhebung von Verkehrs-, Nutzungs-, und Bestandsdaten vor.

Dabei wird trotz der gelockerten Eingriffsschwellen vollständig auf einen Richtervorbehalt verzichtet. Die bezüglich der Sicherungsanordnung nach §§ 100g Abs. 7, 101a Abs. 1 Nr. 3a StPO-E ausgeführten Bedenken gelten entsprechend für alle Maßnahmen, bei denen Daten erhoben werden, die die Erstellung eines Bewegungsprofils ermöglichen. Vor dem Hintergrund der **fortschreitenden Bedeutung des digitalen Raums** ist es umso mehr geboten, bei der Speicherung und Erhebung derartiger Verkehrsdaten eine **lückenlose gerichtliche Kontrolle** zu gewährleisten.

7. Kumulative Eingriffsverstärkung durch das Zusammenwirken nationaler IP-Adressdatenspeicherung und der E-Evidence-Verordnung

Die grundrechtliche Bewertung der geplanten IP-Adressdatenspeicherung darf nicht isoliert auf nationaler Ebene erfolgen. Vielmehr ist sie im Lichte der

unionsrechtlichen Rahmenbedingungen, insbesondere der Verordnung (EU) 2023/1543 über Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel (sog. E-Evidence-Verordnung), zu betrachten. Erst in dieser Gesamtschau wird die tatsächliche Eingriffsintensität der vorgesehenen Regelungen deutlich.

Die geplante IP-Adressdatenspeicherung schafft einen dauerhaft verfügbaren, flächendeckenden Datenbestand, der – wie ausgeführt – bereits bei niedrigen Eingriffsschwellen und ohne Richtervorbehalt für Ermittlungszwecke herangezogen werden kann. Dieser Datenbestand ist jedoch nicht allein für nationale Strafverfolgungsbehörden zugänglich. Durch die E-Evidence-Verordnung wird er zugleich faktisch in einen unionsweiten Ermittlungsverbund eingebettet, der den grenzüberschreitenden Zugriff auf bei deutschen Anbietern gespeicherte Verkehrsdaten erheblich erleichtert.

Zwar enthält die E-Evidence-Verordnung formell keine Verpflichtung zur Einführung neuer Speicherpflichten. Sie entfaltet jedoch eine erhebliche faktische Rückwirkung auf nationale Speicherregime: Je umfangreicher und niedrighschwelliger ein national vorgehaltener Datenbestand ist, desto größer ist zugleich der Kreis potentieller Zugriffe durch Behörden anderer Mitgliedstaaten. Die Eingriffsintensität der nationalen Speicherpflicht erhöht sich damit qualitativ und quantitativ durch die unionsrechtlich eröffnete Zugriffsdimension.

Besonders problematisch ist, dass die E-Evidence-Verordnung auf dem Prinzip der gegenseitigen Anerkennung beruht und nationale Schutzstandards – etwa höhere Eingriffsschwellen, strengere Richtervorbehalte oder besondere Verwendungsbeschränkungen – im Ergebnis unterlaufen werden können.¹ Die in Deutschland gespeicherten IP-Adressdaten werden damit potentiell Ermittlungsmaßnahmen unterworfen, die nach deutschem Verfassungsrecht in dieser Form oder bei dieser Deliktsqualität unzulässig wären.

¹ Vgl. auch die DAV-Stellungnahmen zur VO ([Nr. 42/2018](#)) und zum Durchführungsgesetz (Nr. [87/2024](#) und [42/2025](#))

In der Gesamtschau entsteht so ein kumulativer Grundrechtseingriff, der über die Summe der Einzelmaßnahmen hinausgeht. Die Kombination aus anlassloser bzw. flächendeckender Vorhaltung sensibler Verkehrsdaten, abgesenkten nationalen Zugriffsschwellen und unionsrechtlich erleichtertem grenzüberschreitenden Datenzugriff birgt die Gefahr einer strukturellen Entgrenzung staatlicher Überwachungsbefugnisse. Dies widerspricht den vom Bundesverfassungsgericht und vom Gerichtshof der Europäischen Union entwickelten Anforderungen, wonach Eingriffe in das Telekommunikationsgeheimnis und das Recht auf informationelle Selbstbestimmung nur bei klarer Zweckbindung, strikter Begrenzung auf schwere Straftaten und unter wirksamer richterlicher Kontrolle zulässig sind.

Der Gesetzgeber ist daher gehalten, die geplante IP-Adressdatenspeicherung auch unter Berücksichtigung ihrer unionsrechtlichen Anschlussfähigkeit zu bewerten und wirksame materielle und verfahrensrechtliche Sicherungen vorzusehen, die eine kumulative und grenzüberschreitende Ausweitung der Eingriffe verhindern. Andernfalls droht eine grundrechtlich nicht mehr zu rechtfertigende Verdichtung staatlicher Zugriffsmöglichkeiten auf digitale Kommunikationsspuren nahezu der gesamten Bevölkerung.

8. Gesamtbewertung

Die Neuregelung ersetzt ein abgestuftes, differenzierendes Schutzsystem durch eine einheitliche Eingriffsschwelle. Entgegen der Darstellung im Gesetzentwurf wird das Schutzniveau nicht bewahrt, sondern strukturell eingeebnet. Besonders die gleichzeitige Streichung des Straftatenkatalogs in § 100g Abs. 2 StPO, die Einführung des sog. „Quick-Freeze“ und die Einführung einer mehrmonatigen IP-Speicherungspflicht werden eine starke Verschärfung der grundrechtlichen Belastung nach sich ziehen, deren Konsequenzen in der Gesamtheit schwer vorhersehbar sind. Gleiches gilt für die aufgezeigten Wechselwirkungen durch das Zusammenwirken der nationalen IP-Adressdatenspeicherung und der E-Evidence-Verordnung.

D. Befugniserweiterungen für das Bundeskriminalamt

Bedenken hat der Deutschen Anwaltverein im Übrigen gegen die im vorliegenden Kontext vorgesehenen Befugniserweiterungen für das Bundeskriminalamt.

In Ergänzung zu dem verfassungsrechtlich zweifelhaften § 10a BKAG soll das BKA zunächst in einem neuen § 10b BKAG ebenfalls die Befugnis zur Anordnung von Verkehrsdaten erhalten. Das vermag schon deshalb nicht zu überzeugen, weil das BKA nur in ganz eng beschriebenen Bereichen genuin zur Strafverfolgung sowie zur Gefahrenabwehr zuständig ist. Die Zuständigkeit zur Strafverfolgung ist in § 4 BKAG umschrieben und beschränkt sich im Wesentlichen auf Erscheinungsformen der internationalen Organisierten Kriminalität und des internationalen Terrorismus sowie bestimmte Staatsschutzbereiche. Im Bereich der Gefahrenabwehr zeigt der einschlägige § 5 BKAG eine noch deutlichere Selbstbeschränkung ausschließlich auf den Bereich des internationalen Terrorismus.

Vor diesem Hintergrund soll nach dem Entwurf die Anordnungsbefugnis nach § 10b BKAG-E allgemein auf die Zentralstellenbefugnis des BKA gem. § 2 Abs. 1 BKAG gestützt werden. Faktisch soll es um die Unterstützung der Länderpolizeien in Fallkonstellationen gehen, in denen „die Zuständigkeit einer Strafverfolgungs- oder Polizeibehörde noch nicht erkennbar ist“ (RefE, S. 56). In der Sache bedeutet dies nichts weniger, als dass das BKA zukünftig Sicherungsanordnungen in Bezug auf Verkehrsdaten sogar schon im zeitlichen Vorfeld eines strafprozessualen Anfangsverdachts oder einer konkreten polizeilichen Gefahr tätig werden dürfen. Besonders deutlich wird dieses Konzept in den in § 10b Abs. 1 Nr. 2 und 3 BKAG-E formulierten Anordnungsvoraussetzungen. Diese regeln teilweise nichts anderes als die verfassungsrechtlich bedenkliche und vom Deutschen Anwaltverein wegen Verstoßes gegen Bestimmtheits- und Verhältnismäßigkeitsanforderungen seit jeher kritisierte Eingriffsschwelle der lediglich „drohenden Gefahr“. Diese ist aber – sieht man einmal vom hoch umstrittenen Bayerischen Polizeiaufgabengesetz ab – in den meisten Polizeigesetzen der Länder gerade nicht als Eingriffsschwelle anerkannt, so dass der Bundesgesetzgeber diese Wertentscheidung der Länder unterlaufen und damit in deren Gesetzgebungskompetenz hinsichtlich der polizeirechtlichen Gefahrenabwehr eingreifen würde.

Hinzu kommt, dass es für die Anordnungscompetenz an einem Richtervorbehalt fehlt, obwohl die Maßnahme auf bis zu drei Monate befristet werden darf (§ 10b Abs. 4 S. 1 BKAG-E). Stattdessen soll die Anordnung nach § 10b Abs. 2 BKAG-E durch die zuständige Abteilungsleitung des BKA oder deren Vertretung angeordnet und kann sogar noch auf weitere Bedienstete mit Befähigung zum Richteramt übertragen werden. Ein derartiges Absenken der Qualität präventiven Rechtsschutz wird der Grundrechtsintensität der Maßnahme nicht annähernd gerecht. Der gesamte § 10b BKAG-E erscheint daher zu unbestimmt und sollte im weiteren Gesetzgebungsverfahren ersatzlos gestrichen werden. Dafür spricht auch, dass in der Entwurfsbegründung eine nachvollziehbare Begründung dafür fehlt, warum gerade das BKA eine genuine Kompetenz zur Sicherungsanordnung von Verkehrsdaten benötigt und für seine thematisch beschränkten operativen Befugnisse nicht die geltenden gesetzlichen Befugnisse zur Datenübermittlung genügen.

Entsprechende Einwände sind im Übrigen auch gegenüber der geplanten Erweiterung des ohnehin bereits verfassungsrechtlich bedenklichen § 52 BKAG zu erheben. Konkret soll in einem neuen § 52 Abs. 3 BKAG-E eine Sicherungsanordnung für Verkehrs- und Nutzungsdaten in Bezug auf die Gefahrenabwehraufgaben des BKA im Bereich des internationalen Terrorismus neu geschaffen werden (vgl. RefE, S. 59). Auch hier fehlt es wiederum an einem Richtervorbehalt. Das BKA könnte sich somit in massivem Umfang durch erhebliche Grundrechtseingriffe zu erlangende personenbezogene Daten faktisch weitgehend unkontrolliert selbst beschaffen.

Verteiler

- Bundesministerium der Justiz und für Verbraucherschutz
- Bundesministerium des Innern
- Bundesministerium für Wirtschaft und Energie
- Bundesministerium für Digitales und Staatsmodernisierung
- Ausschuss für Recht und Verbraucherschutz im Deutschen Bundestag
- Ausschuss für Inneres im Deutschen Bundestag
- Finanzausschuss des Deutschen Bundestages
- Ausschuss für Wirtschaft und Energie im Deutschen Bundestag
- Ausschuss Digitale Agenda im Deutschen Bundestag
- Ausschuss für Digitales und Staatsmodernisierung des Deutschen Bundestages
- Arbeitsgruppe Recht der im Deutschen Bundestag vertretenen Parteien
- Arbeitsgruppe Inneres der im Deutschen Bundestag vertretenen Parteien
- Rechtsausschuss des Bundesrates
- Europäische Kommission, Vertretung in Deutschland
- Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
- Landesdatenschutzbeauftragte
- Bundesgerichtshof

- Rechtsausschüsse der Landtage
- Justizministerien und Justizverwaltungen der Bundesländer
- Landesministerien und Senatsverwaltungen des Innern

- Bundesrechtsanwaltskammer
- Bundesnotarkammer
- Deutscher Richterbund, Bund der Richterinnen und Richter, Staatsanwältinnen und Staatsanwälte e.V.
- Deutscher Juristentag
- Bundesverband der Freien Berufe
- Deutscher Notarverein
- Deutscher Steuerberaterverband e.V. Berlin
- Bundesverband der Deutschen Industrie e.V.
- Arbeitsgemeinschaft berufsständischer Versorgungseinrichtungen e.V.
- Deutscher EDV-Gerichtstag e.V.
- GRUR - Deutsche Vereinigung für gewerblichen Rechtsschutz und Urheberrecht e.V.
- Bitkom e. V.
- Deutsche Gesellschaft für Recht und Informatik e.V. (DGRI)
- Gewerkschaft der Polizei
- Deutsche Polizeigewerkschaft im DBB
- Bund Deutscher Kriminalbeamter
- Stiftung neue Verantwortung e.V.
- Deutsches Institut für Menschenrechte
- Gesellschaft für Freiheitsrechte
- Institut für Deutsches und Europäisches Strafprozessrecht
- Deutscher Strafverteidiger e.V.
- Regionale Strafverteidigervereinigungen
- Organisationsbüro der Strafverteidigervereinigungen und -initiativen
- Deutscher Juristinnenbund e.V. (djb)
- Wirtschaftsstrafrechtliche Vereinigung e.V. (WisteV)

- Neue Richter*innenvereinigung e.V.
- Bund Deutscher Kriminalbeamter
- Deutsche Vereinigung für Jugendgerichte und Jugendgerichtshilfen
- Deutscher Juristentag
- Gesellschaft für Freiheitsrechte (GFF)
- Innocence Project Deutschland – Fehlurteil und Wiederaufnahme e.V.
- Kriminalpolitischer Kreis
- Arbeitskreis Alternativ-Entwurf
- ver.di, Bereich Recht und Rechtspolitik
- Strafrechtsausschuss und Strafprozessrechtsausschuss der Bundesrechtsanwaltskammer
- Vors. des Strafrechtsausschusses des KAV und des BAV

- Mitglieder des Vorstandes des Deutschen Anwaltvereins
- Vorsitzenden der Landesverbände des Deutschen Anwaltvereins
- Vorsitzenden der Gesetzgebungsausschüsse des Deutschen Anwaltvereins
- Ausschuss Recht der Inneren Sicherheit des Deutschen Anwaltvereins
- Informationsrechtsausschuss des Deutschen Anwaltvereins
- Strafrechtsausschuss des Deutschen Anwaltvereins
- Geschäftsführender Ausschuss der Arbeitsgemeinschaft Strafrecht des Deutschen Anwaltvereins

- Presse

- NJW
- Frankfurter Allgemeine Zeitung
- Süddeutsche Zeitung
- Berliner Verlag GmbH
- Hamburger Abendblatt
- Der Tagesspiegel
- Der Spiegel
- Juris Newsletter
- JUVE Verlag für juristische Information GmbH
- JurPC
- Netzpolitik.org
- Heise
- LTO
- Neue Zürcher Zeitung
- Frankfurter Rundschau
- Zeit
- beck-online
- Kriminalpolitische Zeitung
- Neue Zeitschrift für Verwaltungsrecht
- Die Öffentliche Verwaltung
- Strafverteidiger-Forum (StraFo)
- Neue Zeitschrift für Strafrecht (NSTZ)
- Strafverteidiger (StV)
- Neue Kriminalpolitik (NK)
- Zeitschrift für Wirtschafts- und Steuerstrafrecht (wistra)
- Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht (NZWiSt)

- Zeitschrift für Rechtspolitik (ZRP)
- Kriminalpolitische Zeitschrift (KriPoZ)
- HRR-Strafrecht
- Zeitschrift für Internationale Strafrechtswissenschaft (ZfIStw)
- Beck Verlag, Deubner Verlag, Juris, LexisNexis, Verlag Dr. Otto Schmidt, Wolters-Kluwe Online, ZAP Verlag